EXHIBIT A

FILED
12/27/2022 1:01 PM
IRIS Y. MARTINEZ
CIRCUIT CLERK
COOK COUNTY, IL
2022CH12414
Calendar, 5
20806317

FILED DATE: 12/27/2022 1:01 PM 2022CH12414

IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

ALAN MURPHY, JR., Individually and on behalf of all others similarly situated, PLAINTIFF, **v.** **LASTPASS US LP and GOTO TECHNOLOGIES USA, INC.,** DEFENDANTS.	2022CH12414 Case No.: Hon. Calendar Courtroom

CLASS ACTION COMPLAINT

Plaintiff Alan Murphy, Jr., individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants LastPass US LP ("LastPass") and GoTo Technologies USA, Inc. ("GoTo"), to seek redress for the defendants' conduct leading up to, surrounding, and following a data vulnerability and breach incident that exposed the personal information of hundreds of thousands of their customers. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

NATURE OF THE CASE

1. Defendant LastPass US LP and GoTo Technologies USA, Inc. (Collectively "Defendants") failed to safeguard the confidential personal identifying information of Plaintiff Alan Murphy, Jr. ("Plaintiff") and millions of individuals ("Class Members" or collectively as the "Class"). This class action is brought on behalf of Class Members whose personally identifiable information ("PII", or "Private

Information") was stolen by cybercriminals in a cyber-attack that accessed sensitive information through the Defendants' computer system.

2. The Defendants' failure to implement or maintain adequate data security measures for personal information directly and proximately caused injuries to Plaintiff and the Class.

3. Defendants failed to take reasonable steps to employ adequate security measures or to properly protect sensitive Private Information despite well-publicized data breaches at numerous businesses and financial institutions in recent years.

4. Despite numerous and high-profile data breaches, Defendants failed to implement basic security measures to prevent unauthorized access to this information.

5. Citizens from across the United States have suffered real and imminent harm as a direct consequence of the Defendants conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure its data systems, as well as the data stored therein, were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard Private Information; and (d) failing to provide timely and adequate notice of the data breach.

6. The Data Breach was the inevitable result of Defendants' inadequate data security measures and approach to data security. Despite the well-publicized and ever-growing threat of security breaches, and despite the fact that data breaches

were and are occurring across numerous industries, Defendants failed to ensure that it maintained adequate data security measures causing the Private Information Plaintiff and Class Members to be stolen.

7. As a direct and proximate consequence of Defendants' negligence, a massive amount of customer information was stolen from Defendant. Upon information and belief, Defendants' Data Breach compromised the Private Information of millions (if not more) of Individuals. Victims of the Data Breach have had their Private Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise been injured.

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

9. Plaintiff, on behalf of themselves and the Class seeks (i) actual damages, economic damages, emotional distress damages, statutory damages and/or nominal damages, (ii) punitive damages, (iii) injunctive relief, and (iv) fees and costs of litigation.

JURISDICTION AND VENUE

10. Jurisdiction over the Defendants is proper under 735 ILCS 5/2-209(a)(l) (transaction of any business within this State), section 2-209(b)(4) (corporation doing

business within this State), and section 2-209(c) (any other basis now or hereafter permitted by the Illinois Constitution and the Constitution of the United States).

11. Venue is proper in this county pursuant to 735 ILCS 5/2-101, because the Defendants regularly does business in this county. 735 ILCS 5/2-102.

12. Pursuant to General Order No. 1.2 of the Circuit Court of Cook County, this action is properly before the Chancery Division of the County Department because it is a putative Class Action.

PARTIES

13. Plaintiff Alan Murphy, Jr. was a resident and citizen of the State of Florida during all times relevant to this complaint.

14. Defendant LastPass is a limited partnership organized under the laws of the State of Delaware with its primary place of business in Massachusetts. Defendant LastPass regularly does business in the State of Illinois.

15. Defendant GoTo is a corporation organized under the laws of the State of Delaware with its primary place of business in Massachusetts. Defendant GoTo regularly does business in the State of Illinois and maintains a registered agent in Illinois.

FACTUAL ALLEGATIONS

A. The Data Breach

16. Defendant LastPass is a software company that provides software to businesses and consumers allowing them to store their passwords and other information. Defendants claimed that their service was secure and that they would

maintain the privacy and security of the Private Information of Plaintiff and the class members.

17. Defendant GoTo is an affiliate of LastPass and also held the information that was entrusted by Plaintiff and the Class Members to Defendant LastPass.

18. In August 2022 Defendants suffered a data that occurred on its computer systems.

19. LastPass initially issued a data breach notice that claimed that several weeks prior unusual activity was detected on their servers but that no customer data was accessed.

20. In September 2022 LastPass issued another notice claiming that it performed a forensic investigation of the data breach and again confirmed that no customer data was accessed.

21. In November 2022 Defendants issued a third notice admitting that the data breach involved customer information but claimed that no passwords were breached.

22. In December 2022 LastPass issued a fourth notice admitting that customers passwords were breached along with substantial amounts of other customer information including payment information and other contact information.

23. Plaintiff's and Class Members' sensitive personal information, which was entrusted to the Defendants, its officials and agents, was compromised, unlawfully accessed, and stolen due to the data breach.

24. As a result of Defendants' actions and/or inaction, Plaintiff and the Class Members were harmed and must now take remedial steps to protect themselves from future loss. Indeed, Plaintiff and all Class Members are currently at a very high risk of misuse of their Private Information in the coming months and years, including but not limited to unauthorized account access including on third-party services and identity theft through use of personal information to open up accounts.

25. In late December 2022, months since the breach occurred, LastPass began notifying consumers of the full extent of the Data Breach.

26. LastPass and GoTo indicated that they had lost control of information it held on to consumers who used the LastPass service while the information was also held by GoTo.

27. On information and belief, even though millions of consumers have had their personal data breached due to the Defendants' actions and inactions, the Defendants have not specifically provided notice to all of these consumers.

28. As a result of the Defendants' failure to properly and timely notify its customers of the full extent of the data breach, members of the class have not had the opportunity to fully protect themselves and modify their passwords and other account credentials.

29. The criminals were able to access Plaintiff's and the Class's personal information because the Defendants failed to take reasonable measures to protect the Personally Identifiable Information they collected and stored. Among other things, Defendants failed to implement data security measures designed to prevent this

attack, despite repeated industry wide warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

30. As a result of Defendants' failure to properly secure Plaintiff's and the Class Members' personal identifying information, Plaintiff's and the Class Members' privacy has been invaded.

31. Moreover, all of this personal information is likely for sale to criminals on the dark web, meaning that unauthorized parties have likely accessed and viewed Plaintiff's and the Class Members' PII.

B. Data Breaches and Industry Standards of Protection of PII

32. Identity theft, which costs Americans billions of dollars a year, occurs when an individual's personal identifying information is used without his or her permission to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, and they typically lose hundreds of dollars.

33. According to the Federal Trade Commission ("FTC"):

> **Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.**

34. The United States Government Accountability Office ("GAO") has stated that identity thieves can use identifying data to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity

theft is the most damaging because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating. Like the FTC, the GAO explained that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

35. Industry Standards highlight several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

36. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

37. Accordingly, federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed in the Data Breach.

38. The FTC has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"). The FTC Report provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their

files, the FTC Report instructs businesses to follow, among other things, the following guidelines:

a. Know what personal information you have in your files and on your computers;

b. Keep only what you need for your business;

c. Protect the information that you keep;

d. Properly dispose of what you no longer need;

e. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and

f. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

39. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

40. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

41. Upon information and belief, the Defendants have policies and procedures in place regarding the safeguarding of confidential information they are

entrusted with, and Defendants failed to comply with those policies. Defendants also negligently failed to comply with industry standards or even implement rudimentary security practices, resulting in Plaintiff's and the Class's confidential information being substantially less safe than had this information been entrusted with other similar companies.

42. The Defendants were aware of the likelihood and repercussions of cyber security threats, including data breaches, having doubtlessly observed numerous other well-publicized data breaches involving major corporations over the last decade- as well as the numerous other similar data breaches preceding those major breaches.

43. In addition to the Defendants' failure to prevent the Data Breach, the Defendants also failed to detect the Data Breach and realize this Private Information remained publicly accessible and unencrypted for a substantial amount of time.

44. Hackers, cyber-criminals, and other nefarious actors, therefore, had sufficient time to collect this Private Information unabated. During this time, the Defendants failed to recognize the failure to protect this Private Information. If the Defendants had quickly detected the Data Breach, this likely would have significantly reduced the consequences of the Data Breach. Instead, the Defendants' delay in detecting the Data Breach contributed to the scale of the Data Breach and the resulting damages.

45. The Data Breach occurred because Defendants failed to implement adequate data security measures to protect its database and computer systems from the potential dangers of a data breach and failed to implement and maintain

reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach.

46. The Data Breach was caused and enabled by the Defendants' knowing violation of its obligations to abide by best practices and industry standards in protecting Private Information.

C. The Data Breach caused Current and Future Harm

47. As a direct and proximate result of Defendants' wrongful disclosure, criminals now have Plaintiff's and the Class Members' Private Information. Additionally, the disclosure of their Private Information makes Plaintiff and Class Members much more likely to respond to requests from Defendants or law enforcement agencies for more personal information, such as bank account numbers, login information or other highly personal PII. Because criminals know this and are capable of posing as Defendants or law enforcement agencies, consumers like Plaintiff and fellow Class Members are more likely to unknowingly give away their sensitive personal and private information to other criminals.

48. Defendants' wrongful actions and inactions here directly and proximately caused the public disclosure of Plaintiff's and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of Defendants' wrongful actions and/or inaction, Plaintiff and Class Members have suffered, and will continue to suffer, damages including, without limitation, expenses for credit monitoring and identity theft

insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

49. As a further result of the data breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

50. Identity thieves can use personal information, such as that of Plaintiff, the other Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. Even basic personal information, combined with other contact information, is very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if some information was not involved in the Data breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access other information, including, but not limited to email accounts, government services accounts, e-commerce accounts, payment card information, and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

51. Defendants were at all times fully aware of its obligations to protect the Private Information of Plaintiff and Class Members. Plaintiff and Class Members would not have entrusted their Private Information to the Defendants had they known that the Defendants would fail to maintain adequate data security. The Defendants were also aware of the significant repercussions that would result from their failure to do so.

52. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. Identity theft victims must spend numerous hours and their own money repairing the impact to their credit.

53. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class Members are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges, identity theft, or other financial loss as a result of the Data Breach.

54. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff, the other Class members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including but not limited to:

a. Theft of their Private Information and financial information;

b. Costs for credit monitoring services; unauthorized charges on their debit and credit card accounts;

c. Unauthorized charges on their debit and credit cards;

d. Injury flowing from potential fraud and identity theft posed by their credit/debit card and Private Information being placed in the hands of criminals and already misused via the sale of Plaintiff and Class members' Private Information on the black market and dark web;

e. Losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. Losses in the form of deprivation of the value of their Private Information;

g. The untimely and inadequate notification of the Data Breach;

h. The improper disclosure of their Customer Data;

i. Loss of privacy;

j. Loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. The loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services.

55. Additionally, even with credit monitoring, the damages of a Data Breach will last much longer since this Private Information cannot be completely removed from the possession of cybercriminals. In fact, it will likely continue to circulate on

the dark web and be sold or traded to other hackers and cybercriminals or identity thieves who will use it to continue to perpetuate fraud against the Class Members.

56. Although the Private Information of Plaintiff and the Class Members has been stolen, Defendants continue to hold Private Information of the affected individuals, including Plaintiff and the Class Members.

57. Particularly, because Defendants have demonstrated an inability to prevent a data breach or stop it from continuing even after being detected and informed of the impermissible dissemination—Plaintiff, the other Class members, have an undeniable interest in ensuring their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further disclosure and theft.

58. Accordingly, Plaintiff on behalf of themself and the Class, brings this action against Defendants seeking redress for their unlawful conduct.

CLASS ALLEGATIONS

59. Plaintiff brings these claims on behalf of the following class:

> **All individuals whose PII was exposed while in the possession of Defendants, or any of its subsidiaries and/or agents, during the Data Breach.**

60. Plaintiff may alter the class definitions to conform to developments in the case and discovery.

61. The proposed class meets all requirements under 735 ILCS 5/2-801.

62. The putative Class is comprised of millions of persons, making joinder impracticable. The joinder of the Class Members is impractical and the disposition of

their claims in the Class action will provide substantial benefits both to the parties and to the Court. The Class can be identified through the Defendants' records or the Defendants' agents' records.

63. The rights of each Class Member were violated in an identical manner as a result of the Defendants' willful, reckless and/or negligent actions and/or inaction.

64. **Numerosity:** Upon information and belief, the Class is so numerous that joinder of all individual plaintiffs would be impracticable. The exact number of members of the Class is presently unknown and can only be ascertained through discovery because that information is exclusively in the possession of Defendants. However, it is reasonable to infer that more than 40 individuals in each class were impacted by the data breach at issue. Members of the Class can be easily identified through Defendants' records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

65. **Commonality and Predominance:** This action involves common questions of law and fact, which predominate over any questions affecting individual members of the Class, including, without limitation:

a. Whether Defendants negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' personal identifying information;

b. Whether Defendants were negligent in storing and failing to adequately safeguard Plaintiff's and Class Members' personal identifying information;

c. Whether Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their personal identifying information;

d. Whether Defendants breached their duties to exercise reasonable care in failing to protect and secure Plaintiff's and Class Members' personal identifying information;

e. Whether by disclosing Plaintiff's and Class Members' personal identifying information without authorization, Defendants invaded Plaintiff's and Class Members' privacy;

f. Whether Plaintiff and Class Members sustained damages as a result of Defendants' failure to secure and protect their personal identifying information.

66. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class they seek to represent, and they intend to prosecute this action vigorously. Plaintiff has retained counsel competent and experienced in consumer class actions and complex litigation. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel and Plaintiff's claims are typical of the claims of the class members.

67. **Appropriateness:** A class action in this case would be appropriate

and superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for the Defendants' wrongful conduct. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the judicial system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

68. Defendants have acted or failed to act on grounds that apply generally to the class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I - NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

69. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

70. Upon Defendants accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendants undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods

to do so. Defendants knew that the Private Information was private and confidential and should be protected as private and confidential.

71. The Defendants owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

72. It was reasonably foreseeable that Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' personal identifying information would result in an unauthorized third-party gaining access to such information for no lawful purpose, and that such third parties would use Plaintiff's and Class Members' personal identifying information for malevolent and unlawful purposes, including the commission of direct theft and identity theft.

73. The Defendants knew, or should have known, of the risks inherent in collecting, storing, and sharing Private Information amongst themselves and the importance of adequate security. Defendants knew of should have known about numerous well-publicized data breaches within the industry.

74. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of the Defendants' failure to secure and protect their personal identifying information as a result of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft herein, insurance incurred in mitigation, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and

other economic and non-economic harm, for which they suffered loss and are entitled to compensation.

75. The Defendants' wrongful actions and/or inaction (as described above) constituted, and continue to constitute, negligence at common law.

COUNT II - INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS AND INTRUSION UPON SECLUSION (ON BEHALF OF PLAINTIFF AND THE CLASS)

76. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

77. Plaintiff's and Class Members' Personal Identifying Information is and always has been private.

78. Dissemination of Plaintiff's and Class Members' Private Information is not of a legitimate public concern; publication to third parties of their personal identifying information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

79. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendants' invasion of their privacy by publicly disclosing their private facts including, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they are entitled to compensation.

80. The Defendants' wrongful actions and/or inaction (as described above) constituted, and continue to constitute, an invasion of Plaintiff's and Class Members'

privacy by publicly disclosing their private facts (*i.e.*, their personal identifying information).

COUNT III - BREACH OF CONTRACT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

81. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

82. Plaintiff and other Class Members entered into valid and enforceable express contracts with the Defendants under which Plaintiff and other Class Members agreed to provide their Private Information to Defendant, and Defendants impliedly, if not explicitly, agreed to protect Plaintiff's and Class Members' Private Information.

83. To the extent the Defendants' obligation to protect Plaintiff's and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring the Defendants to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class Members' Private Information, including in accordance with federal, state and local laws as well as industry standards. Neither Plaintiff nor any Class member would have entered into these contracts with the Defendants without the understanding that Plaintiff's and other Class Members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

84. A meeting of the minds occurred, as Plaintiff and Class Members agreed, among other things, to provide their Private Information in exchange for the Defendants' agreement to protect the confidentiality of that Private Information.

85. The protection of Plaintiff's and Class Members' Private Information was a material aspect of Plaintiff's and Class Members' contracts with the Defendants.

86. The Defendants' promises and representations described above relating to FTC regulations and industry practices, and Defendants' purported concern about its clients' privacy rights became terms of Plaintiff's and Class Members' contracts with Defendants. Defendants breached these promises by failing to comply with regulations and reasonable industry practices.

87. Plaintiff and Class Members read, reviewed, and/or relied on statements made by or provided by Defendants and/or otherwise understood that Defendants would protect their Private Information if that information was provided to the Defendants.

88. Plaintiff and Class Members fully performed their obligations under the implied contract with the Defendants; however, Defendants did not.

89. As a result of the Defendants' breach of these terms, Plaintiff and Class Members have suffered a variety of damages including but not limited to: the lost value of their privacy; not getting the benefit of their bargain with Defendants; the lost difference in the value between the secure services Defendants promised and the insecure services received; the value of the lost time and effort required to mitigate

the actual and potential impact of the data breach on their lives, including, inter alia, to close or modify financial and medical accounts, and to closely review and monitor credit reports and various accounts for unauthorized activity. Additionally, Plaintiff and Class Members have been put at an increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

90. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and fees and costs of litigation.

COUNT IV - BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE CLASS)
(IN ALTERNATIVE TO COUNT III)

91. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

92. At all relevant times, Defendants had a duty, or undertook and/or assumed a duty, to implement a reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to safeguard the PII of Plaintiff and the Class members, and to prevent the unauthorized access to and disclosures of this data.

93. Among other things, Plaintiff and Class Members were required to disclose their personal identifying information to Defendants for the provision of services, as well as implied contracts for the Defendants to implement data security

adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

94. When Plaintiff and Class Members provided their Private Information to Defendants in exchange for Defendants' services, they entered into implied contracts with the Defendants pursuant to which Defendants agreed to reasonably protect such information.

95. By entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

96. Under implied contracts, Defendants and/or their affiliated providers promised and were obligated to protect Plaintiff's and Class Members' Private Information. In exchange, Plaintiff and Members of the Class agreed to turn over their Private Information.

97. The implied contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information, are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' data breach notification letters and Defendants' notices of privacy practices.

98. The Defendants' express representations, including, but not limited to the express representations found in their notices of privacy practices, memorialize and embody the implied contractual obligations requiring the Defendants to

implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

99. Plaintiff and Class Members performed their obligations under the contract when they provided their Private Information in consideration for Defendants' goods and/or services.

100. The Defendants materially breached its contractual obligations to protect the private information Defendants gathered when the information was accessed and exfiltrated during the data breach.

101. The Defendants materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant notices of privacy practices. the Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by their notification of the data breach to Plaintiff and Class Members. Specifically, the Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class Members' private information as set forth above.

102. The data breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

103. As a result of the Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive full benefit of the bargain they entered into, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class Members,

therefore, were damaged in an amount at least equal to the difference in the value between the secure services the Defendants promised, and the insecure services received.

104. Had the Defendants disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff, Class Members, nor any reasonable person would have entered into the aforementioned contracts with the Defendants.

105. As a direct and proximate result of the data breach, Plaintiff and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with the Defendants.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff asks for an award in their favor and against the Defendants as follows:

A. Certifying this action as a class action, with a class as defined above;

B. Designation of Plaintiff as representative of the proposed Class and designation of Plaintiff's counsel as Class counsel;

C. For equitable relief enjoining the Defendants from engaging in the wrongful acts and omissions complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from

failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

D. Awarding compensatory damages to redress the harm caused to Plaintiff and Class Members in the form of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm. Plaintiff and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiff's and Class Members' damages were foreseeable by the Defendants and exceed the minimum jurisdictional limits of this Court.

E. Ordering injunctive relief including, without limitation, (i) adequate credit monitoring, (ii) adequate identity theft insurance, (iii) instituting security protocols in compliance with the appropriate standards and (iv) requiring the Defendants to submit to periodic compliance audits by a third party regarding the security of personal identifying information in its possession, custody and control.

F. Awarding Plaintiff and the Class Members interest, costs and attorneys' fees;

G. Awarding Plaintiff and the Class such other and further relief as this Court deems just and proper.

Respectfully Submitted,

By: /s/ *Bryan Paul Thompson*
One of Plaintiff's Attorneys

Bryan Paul Thompson
Robert W. Harrer
CHICAGO CONSUMER LAW CENTER, P.C.
Cook County Firm No. 62709
33 N. Dearborn St., Suite 400
Chicago, Illinois 60602
Tel. 312-858-3239
Fax 312-610-5646
bryan.thompson@cclc-law.com
rob.harrer@cclc-law.com

Michael Kind, Esq. (*Pro Hac Vice* Forthcoming)
Nevada Bar No. 13903
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, NV 89123
Phone: (702 337-2322
FAX: (702) 329-5881
Email: mk@kindlaw.com

DOCUMENT PRESERVATION DEMAND

Plaintiff hereby demands that defendant take affirmative steps to preserve all recordings, data, documents, and all other tangible things that relate to plaintiff, the events described herein, any third party associated with any telephone call, campaign, account, sale or file associated with plaintiff, and any account or number or symbol relating to them. These materials are likely very relevant to the litigation of this claim. If defendant is aware of any third party that has possession, custody, or control of any such materials, plaintiff demands that defendant request that such third party also take steps to preserve the materials. This demand shall not narrow the scope of any independent document preservation duties of the defendant.

By: /s/ *Bryan Paul Thompson*
One of Plaintiff's Attorneys